MDK 28-NOV-73 11:43 20601

Reply to Jim White's Private Journal Dialog Proposal

I think Jim White's proposal about private journal dialog (IJOURNAL, 20543,1:w) is extremely good, and I would be happy to see it implemented at once.

I have only one additional observation to make: It would be desireable to provide the author with both a capability for appending other idents to the read access list of a Journal document, and a capability for completely "declassifying" the document, at any point in time after it's been journalized. 1

MDK 28-NOV-73 11:43 20601

Reply to Jim White's Private Journal Dialog Proposal

(J20601) 28-NOV-73 11:43; Title: Author(s): Michael D. Kudlick/MDK; Distribution: /SRI-ARC JSP; Sub-Collections: SRI-ARC; Clerk: MDK;

how is this ?

Alex McKenzie [AAM] (BBN)
Jon Postel [JBP] (MITRE)

Telnet and FTP Implementation Schedule Change

We have been contacted by several Telnet implementers and concerned users regarding the scheduled changeover from old to new Telnet. There is a good deal of concern about accomplishing a coordinated changeover especially in light of the potential incompatabilities [RFC 559, NIC 18482]. Therefore the changeover is reformulated as follows.

New Telnet implementations are to be ready 1 Jan 74 (as before), but are to use ICP socket 23 (decimal). That is the server Telnet programs will listen on socket 23, and user Telnet programs will connect to socket 23. It will be useful for the user program to let the user optionally select the server socket, as many user Telnet programs currently do. It will also be useful for implementers to consider a server Telnet program capabable of dealing with both protocols as MIT-DMCG has done [RFC 559]. This will provide an opportunity for testing and debugging the new programs in a way that does not interfere with normal use.

During January we will survey the technical liaisons to determine the status of the Telnet implementations. As soon as we determine that the Telnet implementations have reached a point where the changeover can be made without disruption of user services the technical liaisons will be notified.

In light of this change in the Telnet implementation schedule, the FTP schedule is also modified. New FTP implementations are to be ready by 1 Feb 74 (as before), but will continue to use ICP socket 21 (decimal) until we can determine that a changeover is appropriate.

References:

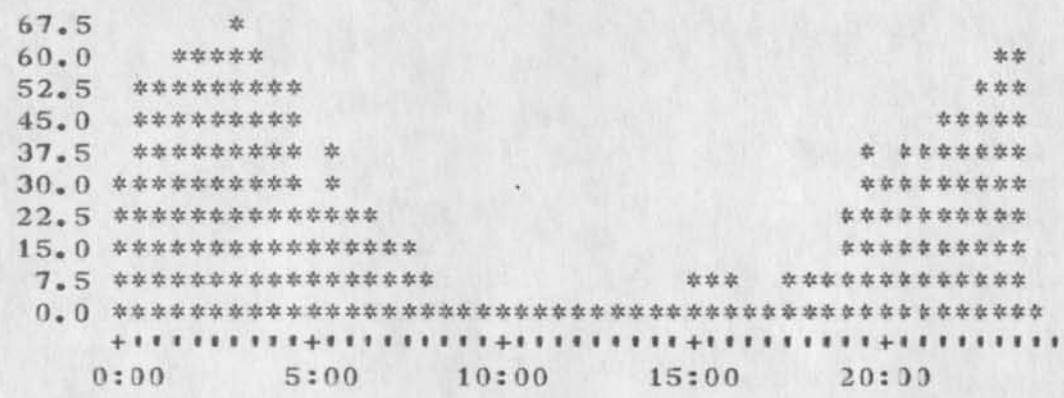
Telnet Protocol NIC 18639

File Transfer Protocol NIC 17759

(J20602) 28-NOV-73 13:22; Title: Author(s): Jonathan B. Postel/JBP;
Distribution: /AAM; Sub-Collections: NIC; Clerk: JBP;

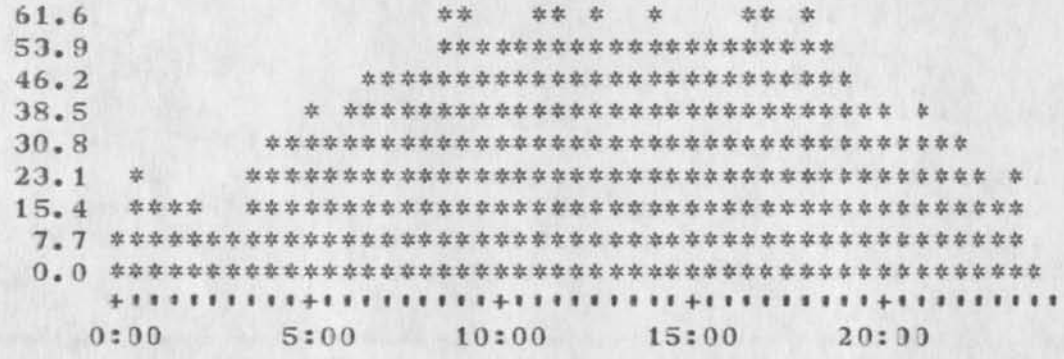
Superwatch Average Graphs for Week of 11/12/73

TIME PLOT OF AVERAGE IDLE TIME FOR WEEK OF 11/12/73
x axis labeled in units of hr:min, xunit = 30 minutes 1



1a

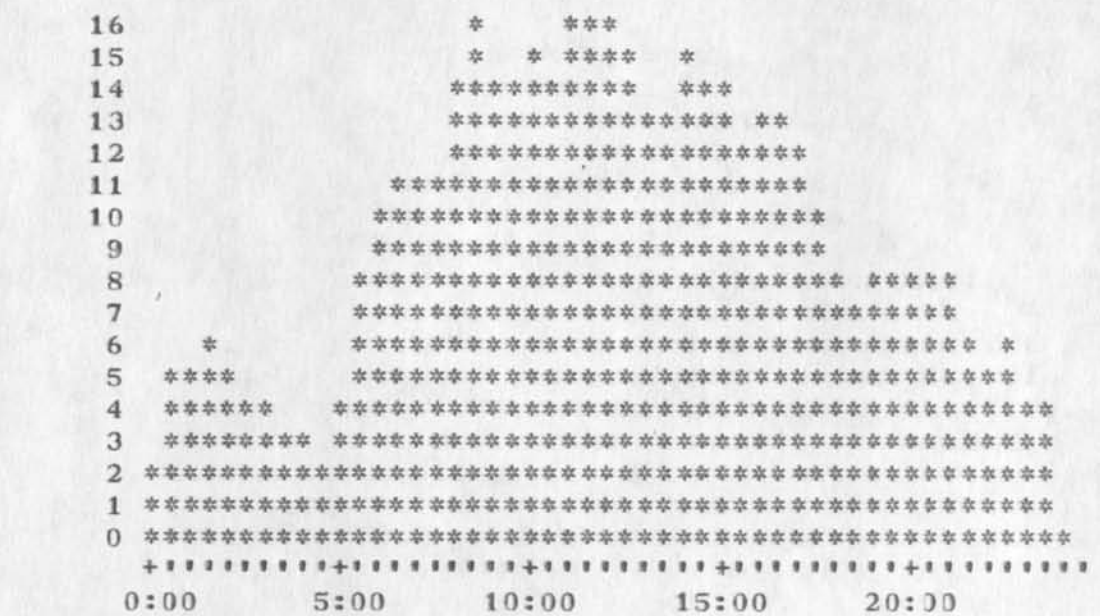
TIME PLOT OF AVERAGE PER CENT OF CPU TIME CHARGED TO USER ACCOUNTS
FOR WEEK OF 11/12/73
x axis labeled in units of hr:min, xunit = 30 minutes 2



2a

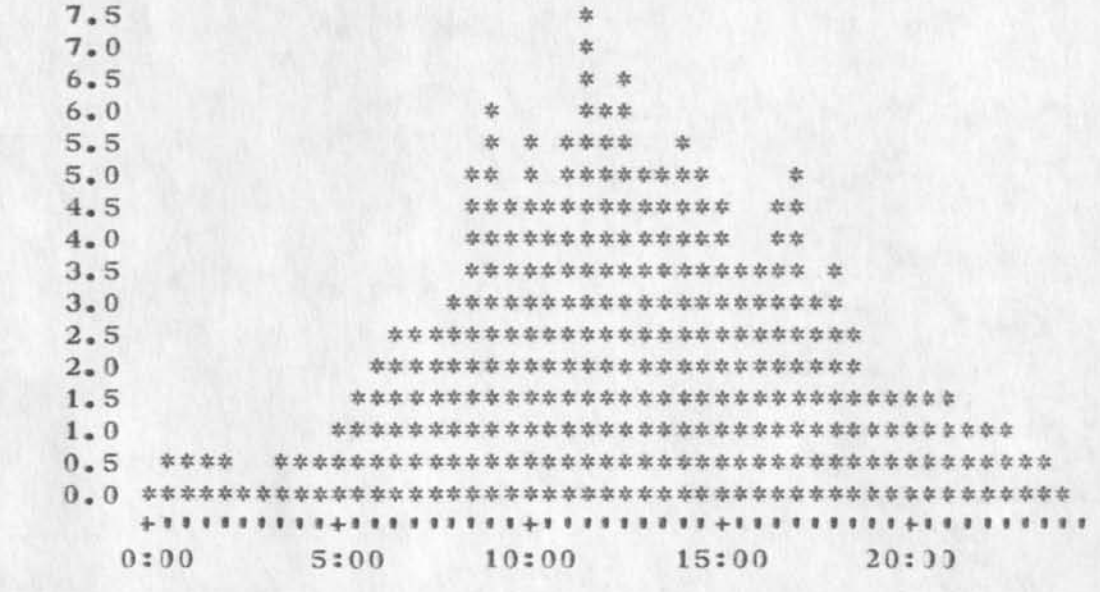
Superwatch Average Graphs for Week of 11/12/73

TIME PLOT OF AVERAGE NUMBER OF USERS FOR WEEK OF 11/12/73
x axis labeled in units of hr:min, xunit = 30 minutes 3



3a

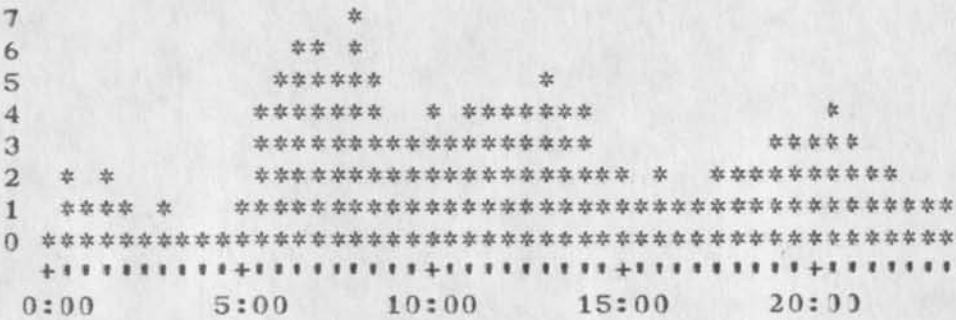
TIME PLOT OF AVERAGE NUMBER OF GO JOBS FOR WEEK OF 11/12/73
x axis labeled in units of hr:min, xunit = 30 minutes 4



4a

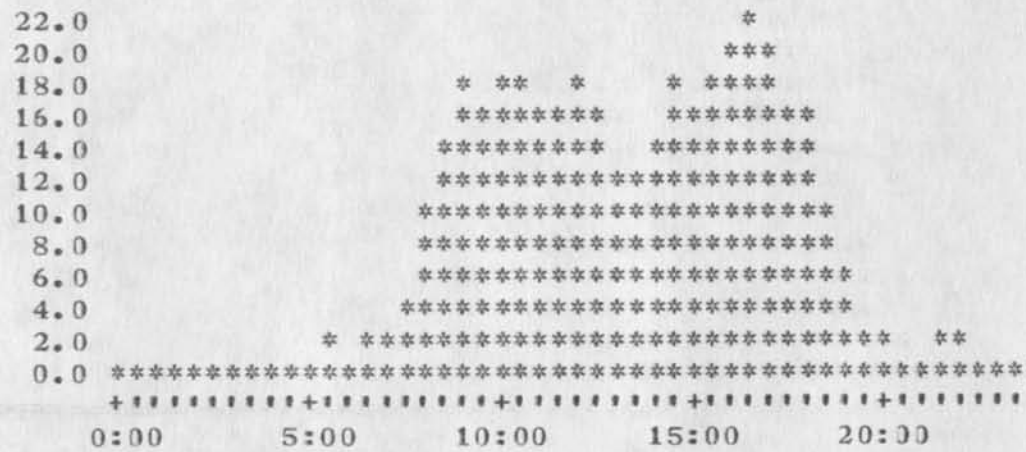
Superwatch Average Graphs for Week of 11/12/73

TIME PLOT OF AVERAGE NUMBER OF NETWORK USERS FOR WEEK OF 11/12/73
x axis labeled in units of hr:min, xunit = 30 minutes 5



5a

TIME PLOT OF AVERAGE PER CENT OF SYSTEM USED IN DNLS FOR WEEK OF 11/12/73
x axis labeled in units of hr:min, xunit = 30 minutes 6



6a

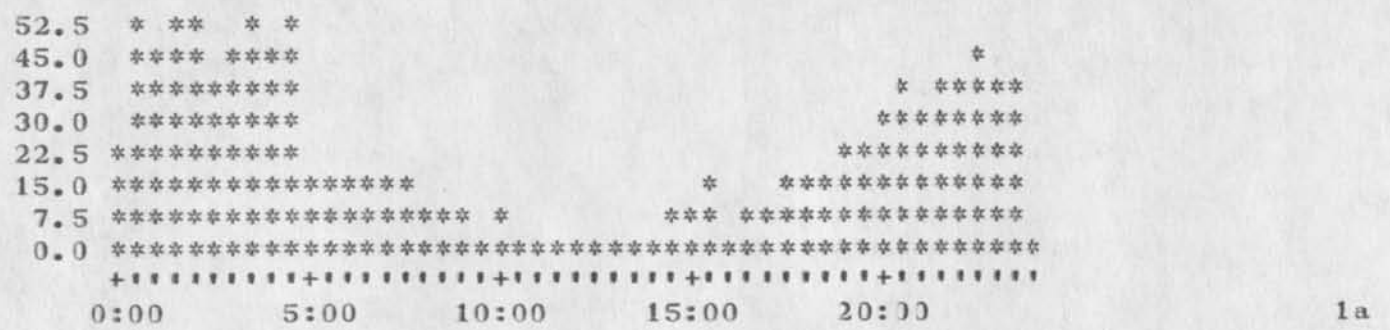
SRL 28-NOV-73 14:08 20603

Superwatch Average Graphs for Week of 11/12/73

(J20603) 28-NOV-73 14:08; Title: Author(s): Susan R. Lee/SRL;
Distribution: /JCN RWW DCE PR JCP DVN JAKE KIRK DLS BAH;
Sub-Collections: SRI-ARC; Clerk: SRL;
Origin: <LEE>WEEK11/12GRAPHS.NLS;1, 20-NOV-73 10:15 SRL ;

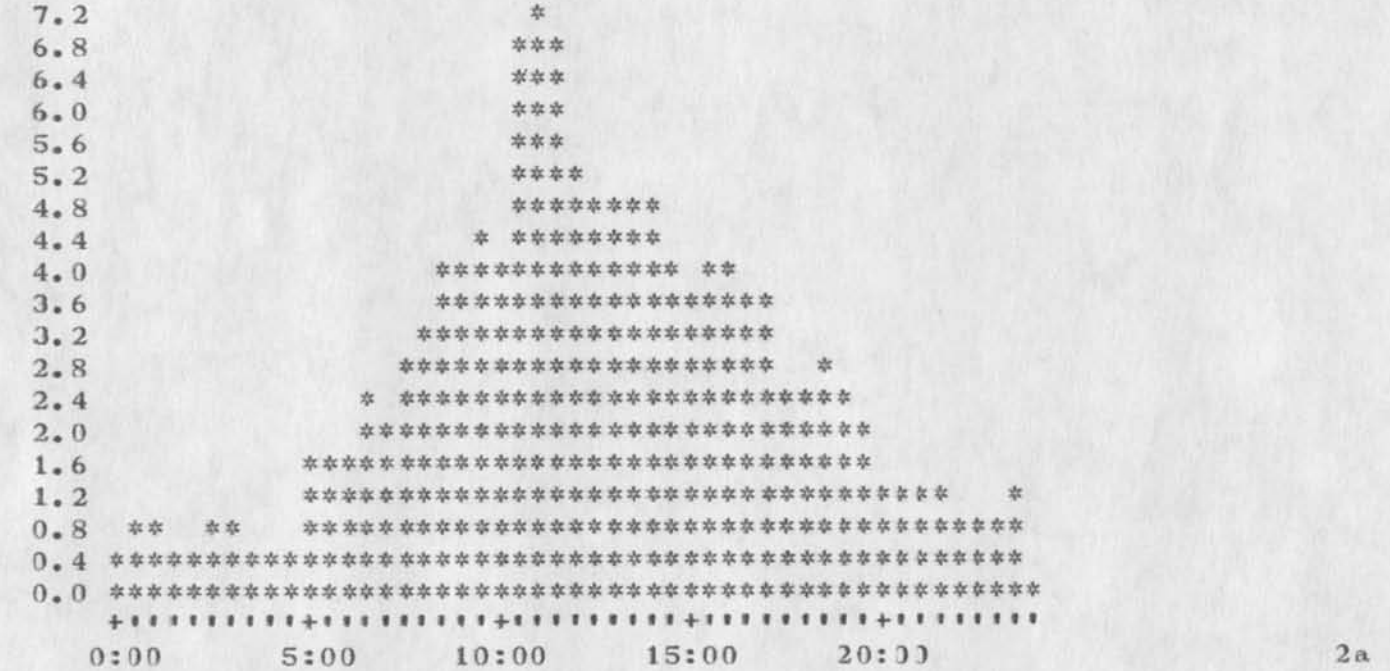
Superwatch Average Graphs for Week of 11/19/73

TIME PLOT OF AVERAGE IDLE TIME FOR WEEK OF 11/19/73
x axis labeled in units of hr:min, xunit = 30 minutes 1



1a

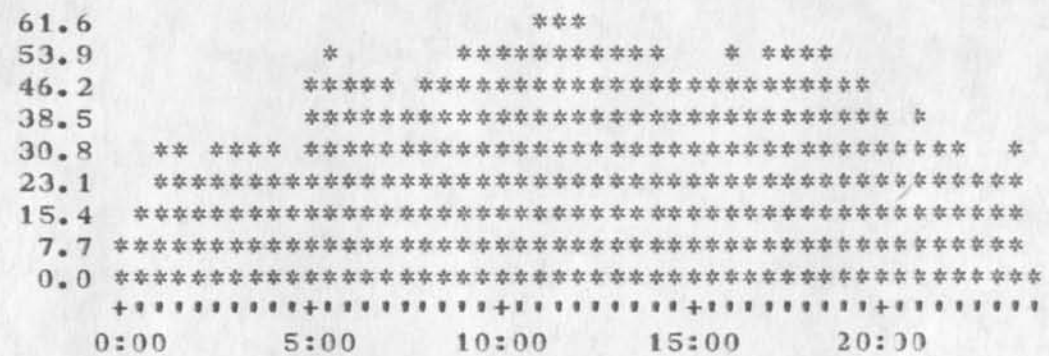
TIME PLOT OF AVERAGE NUMBER OF GO JOBS FOR WEEK OF 11/19/73
x axis labeled in units of hr:min, xunit = 30 minutes 2



2a

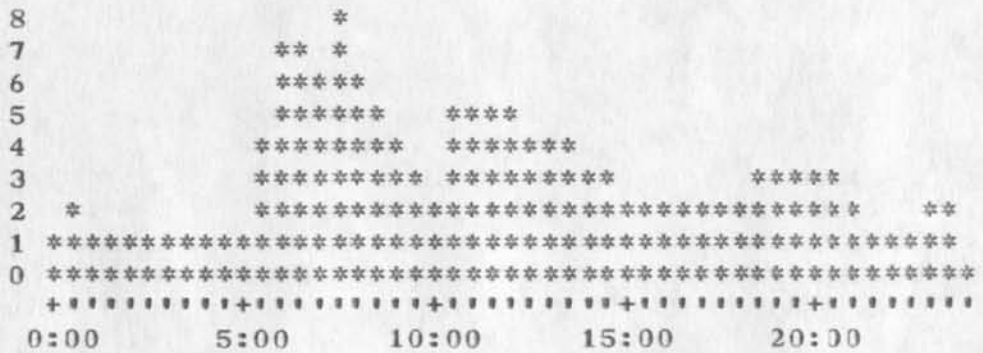
Superwatch Average Graphs for Week of 11/19/73

TIME PLOT OF AVERAGE PER CENT OF CPU TIME CHARGED TO USER ACCOUNTS
FOR WEEK OF 11/19/73
x axis labeled in units of hr:min, xunit = 30 minutes 3



3a

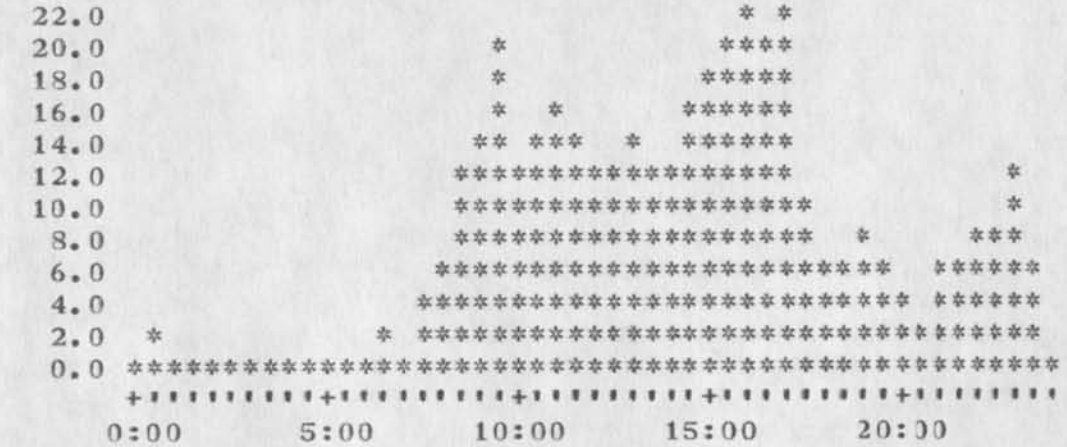
TIME PLOT OF AVERAGE NUMBER OF NETWORK USERS FOR WEEK OF 11/19/73
x axis labeled in units of hr:min, xunit = 30 minutes 4



4a

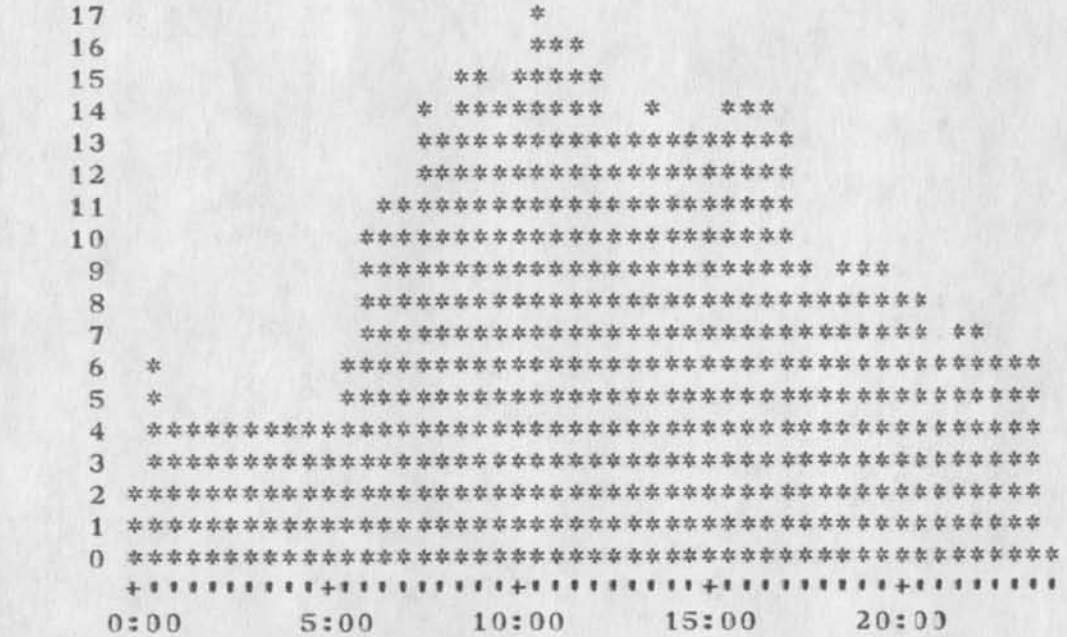
Superwatch Average Graphs for Week of 11/19/73

TIME PLOT OF AVERAGE PER CENT OF SYSTEM USED IN DNLS FOR WEEK OF 11/19/73
x axis labeled in units of hr:min, xunit = 30 minutes 5



5a

TIME PLOT OF AVERAGE NUMBER OF USERS FOR WEEK OF 11/19/73
x axis labeled in units of hr:min, xunit = 30 minutes 6



6a

Superwatch Average Graphs for Week of 11/19/73

(J20604) 28-NOV-73 14:16; Title: Author(s): Susan R. Lee/SRL;
Distribution: /JCN RWW DCE PR JCP DVN JAKE KIRK DLS BAH;
Sub-Collections: SRI-ARC; Clerk: SRL;
Origin: <LEE>WEEK11/19GRAPHS.NLS;2, 28-NOV-73 14:13 SRL ;

EJK 28-NOV-73 14:30 20605

ARPANET Maint.

ISFE (L. COMITO/2242) 21 NOVEMBER 1973 1

ARPA NET MAINTENANCE SUPPORT 2

RADC/ISIM (DR KENNEDY 3

WITH REFERENCE TO THE ARPA NETWORK EQUIPMENT MAINTENANCE SUPPORT PROVIDED BY ISF, IT IS REUESTED THAT YOUR ORGANIZATION PROVIDE SUPPLY INFORMATION RELATIVE TO EACH TYPE OF ARPA TERMINAL. THIS SHOULD INCLUDE AN INVENTORY OF PRESENT STOCK, THE SPECIFIC TYPE OF PAPER, RIBBONS, ETC REQUIRED FOR EACH MACHINE AND ANY OTHER PECULIAR ITEMS THAT MAY BE REQUIRED. 4

ROBERT L. DONDERO 5

ASST CHIEF, R&D COMPUTER FACILITY 6

INFO SCIENCES DIVISION 7

EJK 28-NOV-73 14:30 20605

ARPANET Maint.

(J20605) 28-NOV-73 14:30; Title: Author(s): Edmund J. Kennedy/EJK;
Distribution: /; Sub-Collections: RADC; Clerk: EJK;

ADD 28-NOV-73 15:09 20606

Please send us a copy of NIC # 19933. Since I have the number courtesy of JBP's memory, it should be a large document concerning NGP, by Jim Michener. Thanks ... Buz 1

(J20606) 28-NOV-73 15:09; Title: Author(s): A. D. [Buz) Owen/ADO;
Distribution: /MLK; Sub-Collections: NIC; Clerk: ADO;

ARC3 28-NOV-73 15:15 20607

HAWAII-CON announcement

Can you send me a copy of NIC 16531, the HAWAII-CON announcement?

Thanks, JED

1

HAWAII-CON announcement

(J20607) 28-NOV-73 15:15; Title: Author(s): Guest O. ARC/ARCG;
Distribution: /MLK JED; Sub-Collections: SRI-ARC; Clerk: ARCG;

DHC 28-NOV-73 15:19 20608

l10 file access

Dean -- How does an l10 program specify a file, without using the tbug proc? I want to remove that i/o from user.

Have written my second program, with much easier time of it. Almost getting to like the languaage ( ). D/

1

l10 file access

(J20608) 28-NOV-73 16:19; Title: Author(s): David H. Crocker/DHC;
Distribution: /NDM; Sub-Collections: NIC; Clerk: DHC;

20608 Distribution
N. Dean Meyer,

DHC 28-NOV-73 17:40 20609

L10 user program, for you

Dean -- I have finished my program which creates an index of L10 system procedures (it could also be used for some other things). It assumes a file formatted as SYSGD is. is modifies the whole file, rather than creating a new branch. It formats as follows:

```
Keyword1
   Keyword2(if any)..Key3 Key....Dotsplit Procname (parms)
   Keyword2(diff. proc with same first keyword).....
```

So that the first line of a procedures explanation becomes an index key.
Try the program and see. It is journalized in (20596,). I think it will
make a nice user document. Dave.

DHC 28-NOV-73 17:40 20609

L10 user program, for you

(J20609) 28-NOV-73 17:40; Title: Author(s): David H. Crocker/DHC;
Distribution: /NDM; Sub-Collections: NIC; Clerk: DHC;

DHC 28-NOV-73 13:08 20610

Control-O loop

Occasionally, NLS (NTNLSS) seems to go into an infinite loops after I hit two Control-O's quickly. I have to control-c out and restart. D/ 1

DHC 28-NOV-73 18:08 20610

Control-O loop

(J20610) 28-NOV-73 18:08; Title: Author(s): David H. Crocker/DHC;
Distribution: /BUGS; Sub-Collections: NIC BUGS; Clerk: DHC;

VGC 28-NOV-73 18:45 20611

response to INWG query 11/27

Ira, got your phone message 11-27 "need your exact INWG designation or name" I had trouble interpreting this, but assume you need to know the exact name of INWG. it is IFIP-TC6.1 (International Network Working Group) and I am the chairman of TC6.1. Hope this suffices. See yyou the 18th of Dec. Vint 1

VGC 28-NOV-73 18:45 20611

response to INWG query 11/27

(J20611) 28-NOV-73 18:45; Title: Author(s): Vinton G. Cerf/VGC;
Distribution: /IWC; Sub-Collections: NIC; Clerk: VGC;

DHC 28-NOV-73 20:57 20612

The Life, Death, and Resurection of N*E*T*E*F

How's about our reviving the NETREF effort, but with a somewhat different approach?...:

We design it very carefully, and then prod server sites to build machine readable data-bases that conform. Then we can focus on ways of accumulating the info regularly, getting it reproduced, distributed, etc.

Main problem will be getting info that it up to date. Response: if server doesn't want to provide up-to-date info, that is their problem (or someone who wants to can provide info, as long as it conforms to our format).

Much less work for us. Much more likely to have something happen. The format might even be something USING would like to work on/criticize??

Thoughts? Dave.

1

DHC 28-NOV-73 20:57 20612

The Life, Death, and Resurection of N*E*T*E*F

(J20612) 28-NOV-73 20:57; Title: Author(s): David H. Crocker/DHC;
Distribution: /NJN; Sub-Collections: NIC; Clerk: DHC;

DVN 28-NOV-73 21:15 20613

DRAFT Blurb on COM

Do any of you see any difficulties in sending out a letter such as this to a list of people on the NET who I know are interested in printing?

DRAFT Blurb on COM

One feature of the Online System that we develops at ARC is the capacity to control layout of documents printed from our files. 1

As many of you know it is possible to insert directives in NLS which control the format of the printed page. Normally the pages are printed on a line printer, but it is also possible to print them via a CRT and Computer Output to Micorofilm. From the microfilm can make make xeroxes for prooffing or plates for offset printing. This method of output allows a choice of type faces, proportional spacing with attendent increased density per page, columnation, and a variety of other typographic features. 2

The attached gudie gives instruction for all these features and is itself an example. 3

A commercial COM service,s DSI of Los Angeles prepares the microfilm, prooff copies, or plates from NLS files. DDSI is a few blocks from ISI. We normally creat files on our machine, move them to ISI via FTP where a messanger from DDSI picks them up. DDSI nails the output. The whole cylce takes about a week. 4

DDSI is glad to have buisness from the Net. You may prepare a file through our Output Processor, and send it to DDSI either throught the mail or via ISI. ISI is game to offer this service as long as requests to their operator to handle tape do not become too numerous. If you put your billing address in the file header, DDSI will make proofs, bill you, and mail the proofs to you. Appendix one gives DDSI's current prices. 5

DDSI also prints from a variety of tape formats. Appendix two describes their service in general. If you want to use their COM services without formating via NLS, please get in touch with Robert Spencer at DDSI to arrainge logistics. 6

If you have questions on any of these matters please feel free to ask me or Dean Meyer (Dirk van Nouhuys,415 326-6200, x 3370;DVN@NIC Dean Meyer, 415 326-6200, ex ?; NDM@NIC) 7

Appendix One 8

The present price schedule is as follows: 8a

All initial programming of Photocomposition - negotiable*. 8a1

1. Programming: 8a1a

All initial programming of Photocomposition - negotiable*. 8a1a1

Program modifications to existing applications will be billed on an hourly rate for both machine time and programming time. Upon request for changes, DDSI will supply SRI with a firm quote after evaluation of the effort required. 8a1a2

Machine Time	$350.00 per hour	8a1a2a
Programming Time	25.00 per hour	8a1a2b

2. Output: 8a1b

A. Photocomposed page on 35mm film. 8a1b1

Single font	$ 2.20 page	8a1b1a
Mixed fonts	2.60 page	8a1b1b
Minimum amount	200.00	8a1b1c

B. Copyflo bond proofs 8 1/2 x 11 8a1b2

$.10 per page 8a1b2a

Minimum amount $25.00 8a1b2b

C. Camera ready copy - KP5 8a1b3

$.60 per page 8a1b3a

Minimum amount $25.00 8a1b3b

Thank you for your continued support and interest in our services. 8a1c

Sincerely, 8a1d

Robert Spencer
Marketing Representative
Data Dissemination Systems Inc.
11161 West Pico Boulevard
Los Angeles, Ca. 90064 8a1e

Upon receipt of each new application DDSI will provide a supplemental price quote based on programming analysis application requirements. 8a2

Appendix TWO 9

DRAFT Blurb on COM

October 12, 1973 9a

Dirk van Nouhuys
Dean Meyer
Augmentation Research Center
Stanford Research Institute
Menlo Park, California 94025 9b

Dear Dirk/Dean, 9c

In response to your letter of September 28, I will try to describe to you the services that we can provide to users of the ARPA Network 9d

Our COMP-80 is able to perform 9e

1. Graphics from mag tapes formatted for the FR80 Displayer package. (We can provide the specs needed to generate files in this format). 9e1

2. SC4020 Simulation - High quality with the capability to go "many up" (more than one image per frame). 9e2

3. SC4060 (Meta or IGS) simulation. 9e3

4. Calcomp Plotter simulation (we can handle SOME formats - calcomp seems to have hundreds of formats). 9e4

5. Gerber plotter simulation. 9e5

6. Line Printer simulation with: 9e6

   a. choice of any font (any size between 6pt. and 24 pt.) 9e6a

   b. mono spacing with com fonts, proportional spacing with graphic art fonts (soon). 9e6b

   c. Any set of carriage controls (as long as we know their positions and meaning). 9e6c

   d. EBCDIC, G.E., Honeywell, Burroughs or BCD coding. 9e6d

   e. Many images per frame. 9e6e

   f. Fixed or variable blocking. (Best around block 10) 9e6f

   g. Any line size (up to 255 Characters). 9e6g

   h. Forms overlay. 9e6h

7. Text with illustration merge via our MiSUR package. 9e7

a. MiSUR Phase I provides illustration merge with mono spaced com (stick fonts) only - basically straight print format with illustration merge and forms overlay capability. 9e7a

b. MiSUR Phase II which provides the following: 9e7b

1. Multiple Fonts - The number is limited only by the available disk storage. Font switching "on the fly" is available via carriage control. 9e7b1

2. Change character size, spacing and feed on the fly - Also via carriage control. 9e7b2

3. Monospaced AND proportionally spaced fonts. 9e7b3

4. Horizontal justification (left/right) to a measure specifiable on the fly. 9e7b4

5. Ability to specify (via carriage control) the starting position of a line on a page. [This permits user to specify multi-column formats). 9e7b5

C. MiSUR II has these LIMITATIONS: 9e7c

1. No font switching in mid-line when doing justified text. 9e7c1

2. No stick-font capability graphic arts fonts only. 9e7c2

3. No double-struck (by carriage control) characters in a line in proportially spaced fonts (unless the entire line is double-struck). 9e7c3

4. No vertical justification, leading or pagination on the fly. 9e7c4

We will provide needed user specs upon request. 9f

I hope this is the information you hoped to receive. If you have any questions, I'm sure you'll call. 9g

Sincerely,

Floyd C. Dozier 9h

DRAFT Blurb on COM

FCD/jp 91

DVN 28-NOV-73 21:15 20613

DRAFT Blurb on COM

(J20613) 28-NOV-73 21:16; Title: Author(s): Dirk H. Van Nouhuys/DVN; Distribution: /NDM DCE JCN RWW MDK JCN JAKE COM; Sub-Collections: SRI-ARC COM; Clerk: DVN;

JI 29-NOV-73 05:25 20614

Response to MDK's (20600)

mike: (1) thank you for your response (20600), (2) [20480) was not submitted at a step towards editorial policy, it was submitted to clarify procedures for more efficient development and distribution of the News, (3) I always thought that your Journal system had as a primary element of usage a workshop environment, my item was a first step in an on-going dialog; thus, i must admit i do not understand the statement about prior discussion, (4) To the best of my knowledge, MITRE has the primary responsibility for the development of the ARPANET News but certainly, the effort to remain and grow in viability must be a collaborative effort,

Pursuant to our phone discussion yesterday, I am pleased you like the new format and look forward to its on-line availability through the <help> directory. Also, I very much look forward to our forthcomming discussions in January. Your understanding of my position to not decrease our editorial options unless there is a clear gain to the readership is much appreciated. Warmest regards, ...Jean 1

20614 Distribution

Jeanne B. North, James C. Norton, Douglas C. Engelbart, David H. Crocker, John S. Perry, Steve D. Crocker, Jonathan B. Postel, Mil E. Jernigan, Michael D. Kudlick, Richard W. Watson, Michael A. Padlipsky, Susan S. Poh, Michael D. Kudlick,

JI 29-NOV-73 05:25 20614

Response to MDK's (20600)

(J20614) 29-NOV-73 05:25; Title: Author(s): Jean Iseli/JI;
Distribution: /JBN JCN DCE DHC JSP SDC2 JBP MEJ MDK RWW MAP SSP MDK;
Keywords: newsletter-procedures; Sub-Collections: MITRE-TIP SRI-ARC;
Clerk: JI;

Telnet and FTP Implementation Schedule Change

Alex McKenzie [AAM] (BBN)
Jon Postel [JBP] (MITRE) 1

Telnet and FTP Implementation Schedule Change 2

We have been contacted by several Telnet implementers and concerned users regarding the scheduled changeover from old to new Telnet. There is a good deal of concern about accomplishing a coordinated changeover especially in light of the potential incompatabilities [RFC 559, NIC 18482]. Therefore the changeover is reformulated as follows. 3

New Telnet implementations are to be ready 1 Jan 74 (as before), but are to use ICP socket 23 (decimal). That is the server Telnet programs will listen on socket 23, and user Telnet programs will connect to socket 23. It will be useful for the user program to let the user optionally select the server socket, as many user Telnet programs currently do. It will also be useful for implementers to consider a server Telnet program capabable of dealing with both protocols as MIT-DMCG has done [RFC 559]. This will provide an opportunity for testing and debugging the new programs in a way that does not interfere with normal use. 4

During January we will survey the technical liaisons to determine the status of the Telnet implementations. As soon as we determine that the Telnet implementations have reached a point where the changeover can be made without disruption of user services the technical liaisons will be notified. 5

In light of this change in the Telnet implementation schedule, the FTP schedule is also modified. New FTP implementations are to be ready by 1 Feb 74 (as before), but will continue to use ICP socket 21 (decimal) until we can determine that a changeover is appropriate. 6

References: 7

Telnet Protocol	NIC 18639	7a
File Transfer Protocol	NIC 17759	7b

20615 Distribution

David J. King, Sue Pitkin, Jerry Fitzsimmons, Gloria Jean Martin, Roberta J. Peeler, Craig Fields, Margaret Iwanoto, Dee Larson, Robert E. Doane, Brenda Monroe, Jeanne B. North, Pam J. Klotz Cutler, Stan Golding, Steve G. Chipman, John P. Barden, Martha A. Ginsberg, Shirley W. Watkins, Janet W. Troxel, Connie D. Rosewall, Anita L. Coley, Carol J. Mostrom,
Jeanne B. North, Marcia Lynn Keeney, Travis L. Greening, Brenda B. Epling, Ethyl J. Abeita, Jane A. Bialosky, Marion C. Bedell, Kasee N. Menke, Ruth Ann McDermott, Angie R. Yingling, Michael M. Dervage, Carolyn E. Taynai, Easter D. Russell, Leonard B. Fall, Peggy D. Irving, Roy Levin, M. P. McCluskey, Pitts Jarvis, Barbara A. Nicholas, Jacquie A. Priest, Terence E. Devine, Paul M. Rubin, Paula L. Cotter, O. A. Hansen, Dan Dechatelets, Marcia Lynn Keeney, Margaret A. (Maggie) Bassett, J. A. Smith, Leina M. Boone, Diana L. Jones, Nancy J. Neigus, Terry Sack, Frances A. (Toni) McHale, Lucille C. (Lucy) Gilliard, Ed J. Collins, Gary Blunck, John F. Heafner

NWG/RFC# 593 AAM JBP 29-NOV-73 09:27 20615
Telnet and FTP Implementation Schedule Change

(J20615) 29-NOV-73 09:27; Title: Author(s): Alex A. McKenzie, Jonathan B. Postel/AAM JBP; Distribution: /JBN MLK TLG NSAG; Keywords: protocol implementation schedule telnet FTP; Sub-Collections: NWG NIC NSAG; RFC# 593; Clerk: JBP;

0584-73

Received at NIC 7-DEC-73

20616

Network Working Group
RFC # 594
NIC # 20616

Jerry Burchfiel
BBN-TENEX
10-DECEMBER-73

73 584

Speedup of Host-IMP Interface

I. Introduction

In order to make the full performance capabilities of the subnet available for interprocess communication, the host's IMP interface and the IMP's host interface should operate at the highest speed obtainable.

First, this high throughput will minimize the latency observed when RFNM's, control messages, and NVT (network virtual terminal) characters are queued behind full sized messages. A full-sized message currently ties up a 100 Kb interface for almost 100 Msec. delaying short messages behind it by 100 Msec. Speeding up the host interface to 300 kilobaud will shrink this latency to 30 Msec.

Secondly, this high-speed operation minimizes the time that the IMP buffer and the host core buffer are locked down during message transfer. (One being emptied, one being filled). Being able to dispose of buffers far faster means that many fewer of them will suffice to carry the communications traffic: each buffer can be reused far more often.

Third, high-speed operation makes it possible to improve error control: currently, a destination IMP returns a RFNM after transmitting the first packet of a multipacket message to the destination host. If an error occurs during the transmission of the (up to seven) other packets into the destination host, the source host will not be informed of the error: it has already been given a positive message acknowledgement in the RFNM. The alternative, holding off the RFNM until all packets have been transmitted into the destination host, would add another 80 Msec. to the round trip message - RFNM time with the current 100 kilobaud interface. A higher speed interface will reduce this delayed - RFNM cost to a more acceptable value, making it practical to eliminate this source of undetected message transmission errors.

Fourth, a high speed interface will permit greater host communications bandwidth. (Currently limited to 100 kilobaud). This increase in bandwidth will be essential for communications between hosts at a "network-structured" site, where different hosts on the same IMP are specialized to perform different parts of a computation.

Clearly, any new or retrofitted host interfaces should be very high

speed, and existing host interfaces should be adjusted to operate at their maximum speed, which is in excess of 300 Kilobaud.

II. Experimental Results

In support of the above predictions, the BBN TENEX staff performed an experiment in cooperation with the BBN IMP group to determine how fast the System A (BBN-TENEX) and System B (BBNB) distant interfaces would operate.

Results are as follows:

The Host-to-IMP connection is synchronized by a two-way handshake which has an available burst bandwidth of 1 bit/(2225 nsec + 3 nsec/ft.*<cable length>ft) For our cable length, this results in a bandwidth of 310 Kilobaud.

The IMP-to-Host connection is synchronized by a four-way handshake which has an available burst bandwidth of 1 bit/(1350 nsec + 6 nsec/ft.*<cable length>ft.) which results in a bandwidth of 290 Kilobaud for our installation.

Both System A and System B are now operating at this higher interface speed.

Since the propagation delay time through a distant host driver-receiver pair amounts to 250 nsec, it is expected that local host interfaces (<30ft) can be operated at speeds substantially faster than our 300 Kilobaud.

In addition to the above measurements of hardware speed, new results were obtained in measurements of file transfer performance, i.e. the CPU time and real time used per megabit of information transmitted over the network.

This experiment involved the movement of one-megabit data files to and from an FTP User process in System B communicating with the FTP Server Process in System A. The results are summarized in the following table:

Operation	Byte Size	Type	Bandwidth	User CPU seconds/megabit
Get	8	ASCII	47Kbaud	7.9
Send	8	ASCII	50Kbaud	7.9
Get	32	LocalByte	43Kbaud	1.80
Send	32	LocalByte	38Kbaud	1.70
Get	36	Image	79Kbaud	1.85
Send	36	Image	85Kbaud	.95

The 36-bit bandwidth of around 80 Kbaud is a great improvement from the (typically) 25Kbaud measured before the speedup of the interface hardware. The CPU time use has also decreased somewhat from that

reported in RFC #557 by Barry Wessler: this demonstrates continued improvement of system efficiency between TENEX version 1.31 and TENEX version 1.32.

In conclusion, the BBN-TENEX staff recommends that all host-IMP interfaces in the network be speeded up to the fastest operation obtainable.

RJC 28-NOV-73 05:56 20618

travel vouchers

In regards to travel vouchers, send them to the Branch Office along with your trip repot and IF YOU WISH TO HANDCARRY, PLEASE attach a note saying so and I will call you when they are ready. Is that okay with everybody. The reason for this action is because some people handcarry their travel vouchers over and they never bother doing their trip report. And this FJT do not LIKE 1

20618 Distribution

Larry M. Lombardo, Anna A. Cafarelli, Roberta J. Carrier, Donna R. Robilotta, David L. Daughtry, Richard H. Thayer, Frank J. Tomaini, Mike A. Wingfield, Edmund J. Kennedy, Ray A. Liuzzi, John W. Johnson, Donald Van Alstine, Dean F. Bergstrom, William P. Bethke, Frank S. LaMonica, William E. Rzepka, Rocco F. Iuorno, Frank P. Sliwa, Thomas J. Bucciero, Robert E. Doane, David A. Luther, Roger B. Panara, John L. McNamara, Joe P. Cavano, Duane L. Stone, Marcelle D. Petell, Josephine R. Stellato, Robert K. Walker, Thomas F. Lawrence, James H. Bair,

travel vouchers

(J20618) 28-NOV-73 05:56; Title: Author(s): Roberta J. Carrier/RJC;
Distribution: /RADC; Sub-Collections: NIC RADC; Clerk: RJC;

NJN 29-NOV-73 06:05 20620

NETREF

Dave--
It seems reasonable to resuccitate (sp.?) NETREF--gnosts from the past. I especially like the part where we don't have to do the work. We should decide what real service this is going to provide, i.e., would better cooperation from sites distributing their own documentation alleviate the need? Is this for new or experienced users, or both? How does it relate to what is incuded in the New Users Packet? Should it be included in that packet itself?
I've just raised alot of questins but I don't have any answers yet. I am really wiped out from a bad cold and I can't think straight. I will think about it over the weekend and let you know.
--Nancy

1

20620 Distribution
David H. Crocker,

NJN 29-NOV-73 06:05 20620

NETREF

(J20620) 29-NOV-73 06:05; Title: Author(s): Nancy J. Neigus/NJN;
Distribution: /DHC; Sub-Collections: NIC; Clerk: NJN;

FJT 29-NOV-73 07:08 20621

mess

I would appreciate it if you guys - when you send messages to Frank's directory, please send copy to Carrier's directory as sometimes I don't have a change to log on as both Carrier and Tomaini, if you know what I mean. And if the message should be important, please make sure you do that...Thanks much...Bobbie 1

20621 Distribution

Larry M. Lombardo, Anna A. Cafarelli, Roberta J. Carrier, Donna R. Robilotta, David L. Daughtry, Richard H. Thayer, Frank J. Tomaini, Mike A. Wingfield, Edmund J. Kennedy, Ray A. Liuzzi, John W. Johnson, Donald Van Alstine, Dean F. Bergstrom, William P. Bethke, Frank S. LaMonica, William E. Rzepka, Rocco F. Iuorno, Frank P. Sliwa, Thomas J. Bucciero, Robert E. Doane, David A. Luther, Roger B. Panara, John L. McNamara, Joe P. Cavano, Duane L. Stone, Marcelle D. Petell, Josephine R. Stellato, Robert K. Walker, Thomas F. Lawrence, James H. Bair,

mess

(J20621) 29-NOV-73 07:08; Title: Author(s): Frank J. Tomaini/FJT;
Distribution: /RADC; Sub-Collections: RADC; Clerk: RJC;

RLL 29-NOV-73 08:03 20622

request for network report

This is robert Lieberman from NSRDC. As you probably know we completed a Network Report this past August. At that time we read your draft of 'Computer Network Management Survey'. We were interested in knowing if the report is complete and if so if we could have a copy. Thank you for your time. robbrt lieberman (rll) or nsrdc@sri-arc for sendmsg. 1

20622 Distribution
Ira W. Cotton, Herb M. Ernst,

request for network report

(J20622) 29-NOV-73 08:03; Title: Author(s): Robert N. Lieberman/RLL; Distribution: /IWC HME; Sub-Collections: NIC; Clerk: RLL;

JOC 29-NOV-73 08:07 20623

Marcia,

i wonder if you could update the mailing list to Case-10. There have been a few changes made here, and we have updated the journal master file accordingly. (we have new liasion etc.) Could you (if you are the correct person to talk to) see that these changes are noted. It will help us get information to the correct people here.

thanks,
jim calvin (JOC)

1

20623 Distribution
Marcia Lynn Keeney,

(J20623) 29-NOV-73 08:07; Title: Author(s): Jim O. Calvin/JOC;
Distribution: /MLK; Sub-Collections: NIC; Clerk: JOC;

MDK 29-NOV-73 09:32 20624

Additional Comment on Your Proposal for Private Journal Dialog

Jim ... One additional comment on your file privacy proposal: 1

Suppose I were to load a Journal file that had the "private file bit" set (assuming my ident were in the file's Read List), and assume I then did either of the following nasty things: 2

1) Journalize the same file again, without saying "LIMIT" 2a

2) Output File XXX 2b

It appears from your description in (20543,) that I would be able to destroy the intent of the privacy status, if I did either of these things. 3

It seems desireable that privacy be preserved in each case (certainly at least in the first case). What do you think? 4

Would the problem be solved if both the Read List and the Private File Bit were propagated? 5

20624 Distribution
James E. (Jim) White,

Additional Comment on Your Proposal for Private Journal Dialog

(J20624) 29-NOV-73 09:32; Title: Author(s): Michael D. Kudlick/MDK;
Distribution: /JEW; Sub-Collections: SRI-ARC; Clerk: MDK;
Origin: <KUDLICK>JEW1.NLS;2, 29-NOV-73 09:29 MDK ;

Trip to SADPR, ESD

TRAVEL DUTY REPORT 1

Name(s) of Traveler(s): 1a

Duane Stone 1a1

Name and address of place(s) visited: 1b

MITRE Corp, Mass
Texas Instruments, Waltham, Mass
ESD/MCI, Hanscom Field, Mass 1b1

Period covered 1c

From: 1c1

26 NOV 73 1c1a

To: 1c2

28 NOV 73 1c2a

# of days: 1c3

3 1c3a

Purpose of visit: 1d

To brief SADPR-85 Technology panel on AKW/NLS
To get TI terminals repaired
To determine status of ESD CAI effort with BBN 1d1

Persons contacted: 1e

MITRE--the SADPR-85 technology panel
TI--Dave Doane
ESD--Sylvia Mayer 1e1

Minutes available? (yes or No--if yes when and where): 1f

The SADPR briefing/demo of NLS was video taped. We can get copies of the tape by telling MITRE the kind of video recorder/player we have. (the same is true for other briefers.) 1f1

Contract Number(s): 1g

N/A 1g1

Trip to SADPR, ESD

Project Number: 1h

9991SA85 1h1

Task Number: 1i

N/A 1i1

Commitments made? (yes or no): 1j

no 1j1

Follow up requirements? (yes or no--if yes complete next 3 items) 1k

Date Required: ASAP 1k1

Responsible agency or individual: ISIM 1k2

Action Item: Get copies of Bair's report to SADPR panel 1k3

Summary of events: 1l

The NLS briefing went smoothly--about 15 people in the audience. I did less demoing than I originally thought I might, but did show them the NIC as well as NLS. My offer to delve further into the NIC or NLS after the briefing, was not accepted by anyone at the briefing (perhaps because it was lunch-time). There were questions at the end concerning the cost of the technology, its acceptance by people and programmer aids that it might offer. 1l1

I delivered two defective TI-725 terminals to the Waltham office. They were repaired under warrenty at no charge and I brought them back with me. All of this is in defiance of regulations, but saved about two months and was considerably cheaper. 1l2

I talked briefly with Sylvia Mayer, with regards to her contract with BBN (which will be applying the SCHOLAR CAI package to the teaching of NLS). They have just gotten under contract. The BBN guys are excited at the prospect of tying SCHOLAR into NLS ..anxious to get started. This effort will result in a 3 hour teaching session on SCHOLAR and a primer to introduce NLS to the beginner. If it looks good, they will interface it to NLS in a subsequent effort and expand the coverage. They could now increase the coverage and speed up the effort somewhat, if we were to give them extra money..This was not the case when we talked to them this summer, but they have since hired additional experienced personnel. We (John

McNamara and I) did not encourage them to submit a proposal to this effect; in light of our current money crunch One of the team is a user of NLS, and will be looking at RADC files, prior to visiting RADC, to determine how we now use the system. 1l3

Date: 1m

29 NOV 73 1m1

Symbol: 1n

ISIM 1n1

Traveler: 1o

Duane Stone 1o1

20625 Distribution

Frank J. Tomaini, Edmund J. Kennedy, John L. McNamara, Dirk H. Van Nouhuys, James H. Bair,

DLS 29-NOV-73 10:25 20625

Trip to SADPR, ESD

(J20625) 29-NOV-73 10:25; Title: Author(s): Duane L. Stone/DLS;
Distribution: /FJT EJK JLM DVN JHB; Sub-Collections: RADC; Clerk: DLS;
Origin: <STONE>TRIP.NLS;2, 29-NOV-73 10:21 DLS ;

JHB 29-NOV-73 11:02 20626

New Directory at RADC for MAW

Mike A. Wingfield now has a directory and may be sent Journal ident = MAW) and sndmsg communications. Welcome aboard Mike 1

20626 Distribution

Larry M. Lombardo, Anna A. Cafarelli, Roberta J. Carrier, Donna R. Robilotta, David L. Daughtry, Richard H. Thayer, Frank J. Tomaini, Mike A. Wingfield, Edmund J. Kennedy, Ray A. Liuzzi, John W. Johnson, Donald Van Alstine, Dean F. Bergstrom, William P. Bethke, Frank S. LaMonica, William E. Rzepka, Rocco F. Iuorno, Frank P. Sliwa, Thomas J. Bucciero, Robert E. Doane, David A. Luther, Roger B. Panara, John L. McNamara, Joe P. Cavano, Duane L. Stone, Marcelle D. Petell, Josephine R. Stellato, Robert K. Walker, Thomas F. Lawrence, James H. Bair, James C. Norton, Dirk H. Van Nouhuys,

JHB 29-NOV-73 11:02 20626

New Directory at RADC for MAW

(J20626) 29-NOV-73 11:02; Title: Author(s): James H. Bair/JHB;
Distribution: /RADC JCN(info) DVN(info); Sub-Collections: SRI-ARC RADC;
Clerk: JHB;

L10 Answers

Response to (20547,) and (20609,)

L10 Answers

Dave:
If you initialize a string variable (in the declaration) to a specific string, the maximum length of the variable is the length of that string. If you declare the string variable with its maximum length in square-brackets, the contents of the string are NOT initialized (to NULL or anything else); it is likely to be garbage. Initialization must be done as a seperate operation (*str* ← NULL; or str.L ← 0;). Yes, those are your only two choices. 1

There are a number of ways you may get a handle on a file without asking the user to bug it: 2

If you know what file you want, you may open the file with the following steps: 2a

```
LOCAL stid;                                                    2a1

LOCAL STRING str[50];                                          2a2

stid ← orgstid;                                                2a3

*str* ← "<DIRNAME>FILENAME.NLS" ;                              2a4

stid.stfile ← open( 0,$str);                                   2a5
```

If you want the stid of the pointer at the time of the last Command Accept, you may get it by: 2b

```
LOCAL da, stid;                                                2b1

REF da;                                                        2b2

&da ← dsparea( lcda( ) );                                      2b3

stid ← da.dacsp ;                                              2b4

stid.stpsid ← origin ; %optional move to origin of file%       2b5
```

Good luck. Let me know if this answer is or is not sufficient, and if there is any way I can help further.
--Dean 3

20627 Distribution
David H. Crocker, Joe P. Cavano, Stephen R. Wilbur,

L10 Answers

(J20627) 29-NOV-73 11:45; Title: Author(s): N. Daan Meyer/NDM;
Distribution: /DHC JPC(fyi) SRW(fyi); Sub-Collections: SRI-ARC; Clerk:
NDM;
Origin: <MEYER>TEMP.NLS;1, 29-NOV-73 11:43 NDM ;

Don:
In L10, when you declare a string variable with its maximum length,
e.g. DECLARE STRING str[100];
does L10 initialize the actual length (str.L) to zero? If not, that would be a nice feature. --Dean 1

20628 Distribution
Don I. Andrews,

(J20628) 29-NOV-73 11:56; Title: Author(s): N. Dean Meyer/NDM;
Distribution: /DIA; Sub-Collections: SRI-ARC; Clerk: NDM;

Doug: Due to my confusion and negligence, your encrypting program was never incorporated into the User Programs Library. The problem was that I could not find the NLS file. If you help me one more time (by giving me or Jeff the name if it was archived...) I promise not to loose it Thanks. I'll be talking to you soon. I should be done with school on the 14th. -Dean 1

20629 Distribution
Douglas C. Engelbart,

(J20629) 29-NOV-73 12:07; Title: Author(s): N. Dean Meyer/NDM;
Distribution: /DCE; Sub-Collections: SRI-ARC; Clerk: NDM;

NDM 29-NOV-73 12:18 20630

Re (20579,): Final Report

Dick: Your plans for the Final Report seem like a very good way to approach the problem. [I'm sure you considered the benefits of involving everyone in the effort.] I would be plased to help in any way that I can. Perhaps the collection of files could be easily published using a format in the Output Processor Format library or by developing one and placing it in the library. More on that at your request. 1

20630 Distribution

Richard W. Watson, James C. Norton, Douglas C. Engelbart, Dirk H. Van Nouhuys,

NDM 29-NOV-73 12:18 20630

Re (20579,): Final Report

(J20630) 29-NOV-73 12:18; Title: Author(s): N. Dean Meyer/NDM;
Distribution: /RWW JCN(fyi) DCE(fyi) DVN(fyi); Sub-Collections: SRI-ARC;
Clerk: NDM;

RBP 29-NOV-73 12:31 20631

FY74 PMP TASK 09 SECURITY

THis is the edited version of the FY74 write-up for the PMP.

9. AUTOMATIC DATA PROCESSING (ADP) SYSTEM SECURITY 1

9.1 INTRODUCTION 2

9.1.1 Purpose and Goals: The purpose of this program is to define and develop a comprehensive set of techniques for safeguarding classified information processed by military computer systems. The goal is to provide Air Force computer users with the ability to share electronic data processing (EDP) systems and the information therein as dictated by operational requirements, with the assurance that classified information stored and processed will receive appropriate protection. 3

9.1.2 Potential: Effective security techniques for computer systems will provide the means for protecting classified information while satisfying user requirements and making economical use of EDP equipment. Air Force EDP managers will have for the first time the ability to provide the users with on-line access to only that information in a computer system that the users have a need to know. 4

By providing these security techniques, we can: 4a

a. Satisfy the operational and security requirements of a number of planned Air Force systems that are now technically infeasible (i.e., Air Force Data Services Center (AF/DSC) open-secure computer system discussed below). 4b

b. Assure in advance of implementation that it will be possible to certify as effective the security controls provided by a system. 4c

c. Eliminate the costs now incurred by separating in time or space the computer processing of workloads at differing classification levels. 4d

d. Eliminate the costs of communications security equipment now provided for terminals that access unclassified information stored in computers that handle classified data. 4e

e. Reduce significantly the costs of communications security equipment at a central computer that supports many terminals processing classified data. 4f

f. Reduce significantly the cost of securing remote terminals that must process classified data. 4g

g. Provide more effective support for computer users who must handle partially or totally classified data bases. 4h

9.1.3 Program Genesis: The advent of computers capable of supporting several users in a time-shared or multiprogrammed mode has made critical the problem of safe-guarding classified information processed by computer systems. This problem becomes particularly severe in "open" systems where classified and unclassified information must be processed simultaneously and support must be extended to remote terminals in unsecured areas. Present techniques are inadequate to insure that requirements for such secure processing are met, and yet a mode of secure resource-shared operation is increasingly often required by Air Force computer users. 5

Commercial computer hardware and software (such as that for the World Wide Military Command & Control (WWMCCS)) have serious security inadequacies. Just as the military must augment commercial communication equipment for communications security, similarly specific techniques, will be required for computer security. As indicated in the report of the Command & Control Information Processing for the 1980's (CCIP-85) study group, the lack of such techniques continues to be a major roadblock to effective application of computers in the Air Force. 6

Electronic System Division (ESD) involvement in a number of computer systems for classified processing has accentuated the need for improved computer security technology. Since 1970 ESD has had a continuing effort to support the AF/DSC at the Pentagon in their modernization program. This effort included an analysis of security vulnerabilities, identificaaion of security controls applicable to the existing HIS-635 (GCOS III) system, and support in the acquisition of a new computer system, MULTiplexed Information and Computing System (MULTICS). However, technology advances are needed in order to meet open system requirements, and AF/DSC is potentially a major beneficiary of this development program. 7

In support of the Arnold Engineering Development Center ADP upgrade, multi-level secure processing requirements received major attention. Multi-level computer security is a significant design constraint in the on-going design of the Military Airlift Command Integrated Management System (MACIMS). The Space Automated Telecommunications Information Network (SATIN) system for the Strategic Air Command (SAC) also presents significant multi-level computer security problems. 8

9.1.4 Related Programs: Computer security is a problem of considerable interest throughout the Department of Defense (DOD). However, no coordinated program is now underway to develop integrated solutions to Air Force problems. 9

a. Relationships with other Air Force Programs. Rome Air Development Center (RADC) has performed several studies of security measures in data management systems (DMS's), and is expected to lead the secure DMS efforts of this program. 9a

A number of planned Project 85 engineering developments are related to this program. The results of the program in classified material destruction and denial will use the ADP facility and complement the results of this program by providing improved security for storage media. The program in standards for ADP security will provide guidance in system requirements, implementation, and testing techniques. The WWMCCS II preparation program requires the results of this program to assure security of the planned WWMCCS II computers. 9b

The Secure Telecommunications Terminal being developed under the direction of ESD/DCW will make available techniques and some hardware for a secure user terminal and crypto concentrator. This program will use Secure Telecommunications Terminal results where possible, but must adapt them to the needs of the interactive computer user. 9c

Results of the ESD/MITRE technology base program in secure on-line processing will be applied as appropriate to the front-end processor phase of the development. 9d

b. Relationships with other than Air Force Government Programs. 9e

Defense Intelligence Agency (DIA) has conducted useful studies of security in its existing Defense Intelligence Agency On-Line System (DIAOLS). These studies have shown many of the weaknesses that can be found in a secure system based on most current hardware and software. However, they do not provide positive direction for the development of a secure system for use in an open environment. 9f

National Security Agency (NSA) has a newly established computer security division that is investigating a number of computer-related security problems. NSA is expected to take a leading role in the communicatons security portions of this program, and has coordinated on an earlier draft of this program plan. 9g

Advanced Research Projects Agency (ARPA) sponsors research in new computer architectures for security (the PRIME project at the University of California at Berkley) and is funding teams that attempt to break or penetrate the security controls of existing systems (at Rand Corporation and Lawrence Livermore Laboratories). ARPA has coordinated an earlier draft of this plan. 9h

9.2 ANALYSIS AND TECHNICAL APPROACH 10

9.2.1 Technical Background: Contemporary computer systems use large complex operating system software to provide the functional capabilities expected by modern users. Security control features tend to be dispersed throughout this software , often in subtle and non-obvious ways. Large portions of this system software (typically on the order of a hundred thousand instructions) can potentially access any information in the system for any user. An underlying problem is achieving reasonable confidence that all of this complex software in fact restricts each user's access to just authorized information and maintaining this confidence as the system is modified for new versions and local adaptations. 11

One of the most difficult computer security problems is protecting classified information in a multi-user computer system that has remote terminals without secure communications --an "open" computer system. Providing acceptable protection in an open system is particularly difficult because the unsecured communications give a remotely located intruder an easy way to make sophisticated (viz. computer-aided) attempts at unauthorized access with little risk of apprehension. The crucial consideration in an open system is the security control provided by the hardware and operating system of the central computer. 12

In about 1965, ARPA-sponsored research into multi-user computer systems considered existing information protection capabilities and concluded that contemporary computers required both hardware and software modification to provide adequate protection for the needs of commercial users (e.g. service bureaus). A joint effort of Massachusetts Institute of Technology, General Electric and Bell Laboratories modified the GE-635 to form the GE-645 and developed the MULTICS operating system for this hardware to achieve a major improvement in information protection. The "virtual memory" techniques developed in this and related research are promising as solutions to military computer security problems. 13

The Defense Science Board Task Force on Computer Security was formed in 1967 to recommend hardware and software safeguards that would satisfactorily protect classified information in computer systems. Their February 1970 confidential report, "Security Controls for Computer Systems (U)", concluded that a secure open system could not be provided by contemporary technology. They recommended that research and development be pursued to overcome the technology limitations. 14

The CCIP-85 study group report noted that data security techniques developed to date have not been found adequate to meet the needs of command and control data management systems. Development tasks were recommended in the areas of software, hardware, test and validation methodology, and theoretical foundations. 15

The ESD-sponsored Computer Security Technology Planning Study Panel assembled a number of recognized experts in computer science and computer security during 1972. The panel's recommendations for development form the technical basis for this planned program. 16

The MULTICS operating system referred to above has been brought into successful daily operation, demonstrating the viability of virtual machine concepts. More recently, International Business Machines Corp. (IBM) has adapted its hardware and operating system to embody a few of these same concepts. Hardware implementing the required features of memory segmentation and multiple execution states is availlable in sizes ranging from minicomputers to large-scale processors. 17

Some recent efforts at ESD and MITRE have shown potential for a mathematical basis for computer security. Application of general system theory to the modeling of security control systems offers the prospect of a rigorous definition of security and compromise. Proof-of-correctness techniques may allow for the orderly translation of security requirements into operating computer programs. 18

9.2.2 Alternative Approaches: A development program intended to meet the Air Force needs for security controls in computer systems must consider togetther the various aspects of computer security including system design, hardware, software, operational procedures, certification, maintenance, and audit. However, the various alternative approaches are primarily characterized by the approach for the central computer hardware and software. The alternative approaches to accomplishing this effort's objectives are discussed in the following paragraphs. 19

(a) Ad Hoc Addition of Security Controls 19a

This technique involves fixing individual "bugs" and security deficiences in an existing operating system. It has received great emphasis in the past, but has led to few positive results. Because of the elusive nature of the underlying issues of system complexity, in the past a natural reaction of a new system design team faced with a computer security problem has been to "bite the bullet" with a frontal attack on the various symptoms, leaving the basic problems unsolved. Qualified success has been achieved (most notably in intelligence applications) with major expense by severly limiting a system's functional capabilities--for example, providing only a file query capability. For more general capabilities, efforts to secure contemporary hardware and software have primarily served to confirm to members of the particular design team that improved technology is needed. 19b

The typical approach to certifying as secure a system whose security controls are overlaid on conventional hardware and software has been to assemble a test or "penetration" team. Such a team typically examines the innermost details of the "secure system" in a quest for avenues of penetration or compromise. While the team may find (and the developers fix) some holes, there is never a guarantee that the last bug or weak point has been found. The certification certifies only that those problems that have been found did exist. It says nothing about the presence or absence of other potential leaks. 19c

A related weakness of this approach is its sensitivity to the problems of "system maintenance". In particular, fixing one hole does not imply that after a system improvement is introduced, another hole has not been introduced. The typical experience with current operating systems is that each new version released introduces about as many new bugs as it corrects. A primary means of identifying these bugs is through users reporting symptoms of improper operation. Bugs that constitute security holes are particularly difficult to identify because they may have no operational symptoms, and because some users (viz., a penetrator) will not report holes that they discover. 19d

(b) Automated Secure Design 19e

Computer-aided systems for hardware and techniques for highly reliable programming aid in solving the problems of system complexity. Project LOGOS, started in 1969 at Case Western Reserve University is attempting to link these two methods in an integrated design environment. This approach supported by additional theoretical understanding of computer security could provide a significant advance in the design and manufacture of secure computer systems. A main strength of this approach is that security certification is made much easier by the continuity from

**basic understanding of security to final implementation. However, the integrity of a system is based on its total hardware and software being designed, manufactured, and constructed using this automated environment --a major undertaking for a large computer system. Continued basic research is required, but an operating secure ADP system based on this approach is a number of years away. 19f

(c) Internal Encryption 19g

One approach to bypassing some computer security problems is to operate with programs and data enciphered in main and secondary storage. This approach transfers much of the security requirement to the successful protection of the encipherment/decipherment keys for the operating system software. A particularly strong point for this approach is that all physical storage media are unclassified and the entire system can be rapidly declassified (in response to imminent capture in a tactical environment) by simply destroying the various keys. However, the requirement for continuous encipherment/decipherment may represent an enormous processing overhead. Additional basic research is needed to identify practical hardware mechanisms to develop an effective system architecture using these mechanisms, and to evaluate their impact on system efficiencey. 19h

(d) Virtual Memory Techniques 19i

Recent theoretical work (most notably by Dr. Butler Lampson of Xerox) has developed a generalized model for protection systems. It has been shown that the two-dimensional virtual memory addressing scheme of the MULTICS system is a special case of this protection system model. This fact is of particular interest since the MULTICS architecture also includes features to limit the complexity of its access control mechanisms. 19j

A virtual memory provides each individual user an environment essentiallly the same as if he had a dedicated computer containing only those files he was authorized to access. Two major techniques used by MULTICS are "segmentation" and "protection rings." 19k

(1) Segmentation: All addresses for memory references (both data and instruction fetches) explicity specify the file (or "segment") being referenced, as well as the relative address within the file. This two-part addressing approach is distinct from the typical method of using an absolute address or a relative address with respect to some base register. A separate set of "descriptors" for each user determines the files accessible to that user. Special addressing hardware interprets each user's two-part addresses in terms of his own descriptors and, for each memory reference, checks whether the specific (viz., read, write or execute) access is authorized for the referenced file. This technique results in the restriction that any address generated by a user is only interpreted in terms of files authorized for that user. Therefore, erroneous addresses (accidental or otherwise) cannot lead to security violations. 19l

(2) Protection Rings: Multiple levels of privilege (or protection) can be used to separate security related features of the operating system from other protected functions such as scheduling. This multiplicity is in contrast to the two-level (master/slave mode) scheme commonly used. With segmentation the security functions of the operating system can primarily be a few well-defined operations associated with maintaining the descriptors used by the segmentation hardware. By segregating these security features as a "kernel" into the most privileged or protected ring , the system can insure that errors in the major portion of the operating system software cannot lead to compromise of information. 19m

The current commercial Honeywell MULTICS system for the HIS-6090 has demonstrated a high degree of information protection and privacy. However, some refinements to the existing implementation are needed for military security applications, at least in open systems. 19n

9.2.3 Technical Achievements Planned: The approach selected for this development plan is 9.2.2(d) above - to build on the virtual memory techniques discussed above. Since this approach is based on concepts already shown to be technically and economically feasible, the planned development concentrates on applying them to satisfy USAF computer security requirements. 20

To provide a complete and cohesive set of techniques responsive to Air Force computer security requirements, the planned program includes not only central computer developments, but also the user interface elements needed to make secure computing practical and available. The program comprises four sub-tasks dealing with the central computer and its operating system software, a front-end processor/crypto multiplexer, secure terminals for office use, and application engineering of the overall system. Each sub-task includes four phases covering design, implementation, integration, and test and evaluation. 21

9.2.3.1 Central Computer and Operating System 22

The paragraphs above have discussed central computer security techniques at some length. The theoretical and practical developments discussed under the virtual memory alternative, as well as the recent work mentioned under 9.2.1 above provide ample evidence that a secure central computer system can be produced by pursuing this alternative. 23

9.2.3.2 Front-end Processor/Crypto Multiplexer 24

Modern computer systems that support multiple remote terminals almost always include a small front-end processor dedicated to handling communications tasks. (Examples include the IBM 3705, HIS Datanet-355, Univac Communications Symbiont Processor (C/SP), and (former) RCA1600). A front-end processor serving a secure computer system could be expected to communicate with both cleared and uncleared terminals, and to have powerful access to the central computer's main memory. Thus the front-end processor, like the central computer, must be certifiably secure. 25

In today's systems, each communications circuit handling classified information requires a cryptographic device at the central computer site and another at the terminal site. For a large system, the number and cost of central site cryptographic devices can become very large. An alternative being explored under the Secure Telecommunications Terminal project (see related effort) would have one cryptographic device serve a number of terminals, under the control of a communications processor. Like the front-end processor mentioned above, the crypto device central processor has the ability to mix classified and unclassified data, and therefore must be secure. 26

The front-end processor/crypto multiplexer sub-task is directed toward providing a secure minicomputer communications processor suitable for the front-end and crypto control functions described above. Investigations in the ESD/MITRE tech base program have shown that the virtual memory techniques planned for the central computer apply to a communications processor. Thus this sub-task will be conducted in parallel with the central computer sub-task and will apply its results to the communications computer developments. 27

9.2.3.3 Secure Terminals 28

A major expense associated with the use of remote terminals to process classified data has been providing communications security devices for the terminals and providing physical protection for the security devices. The purpose of this sub-task is to provide an economical (of the order of $3000) secure terminal for use in an office envirnoment. Preliminary developments in this direction (but for another application) have been undertaken by the Secure Telecommunications Terminal program. This sub-task will apply the results of that program to a secure interactive computer terminal. The terminal will be designed to operate with the crypto multiplexer developed by the previous sub-task. 29

9.2.3.4 Application Engineering

To interface the basic central computer system with Air Force users, some specialized software will be required. This software will perform security related functions, but not be part of the security kernel mentioned above. Included in the application engineering area are data management tools and security officer surveillance interfaces. Both sets of tools can benefit from the basic virtual memory and descriptor concepts discused above. Ongoing RADC efforts in secure data management will provide initial direction for this sub-task.

9.2.4 Progress In the exploratory development program, the design of a security kernel for a minicomputer (Digital Equipment Corp. PDP-11/45) has been accomplished by MITRE Corporation. This design was based upon a finite state mathematical model, also developed by MITRE. The system design is directed toward a secure front-end processor and a query system for a secure multi-level data base.

Abstract modeling efforts accomplished by ESD and Case Western Reserve University using a "layered" modeling approach have resulted in design technology required by AF/DSC MULTICS for secure multi-level information processing in a beneign environment. Their modeling efforts are continuing and will have application to the prototype secure central computer development.

9.2.5 Review and Organization: This program involves in-house management, MITRE systems engineering and technical direction, and subsystem development by contractors and other government agencies. Key milestones occur at the end of each phase of each sub-task, as security certification criteria are developed and the validity of the approach is confirmed.

9.3 DEVELOPMENT AND TEST PLAN

9.3.1 Discussion of Development Efforts: Each sub-task under the planned program includes design and implementation phases. Integration and testing and evaluation are required both for the products of individual sub-tasks and across sub-tasks.

9.3.1.1 Central Computer and Operating System

a. In the first or design phase, an abstract model of a secure descriptor-based computer and operating system will be developed. The purpose of this model is to define data bases, modules, and interfaces necessary to maintain the integrity of the segment descriptors. In order to clearly understand the security sensitivities, this model will carefully distinguish operations that need only read from those that must modify descriptors and related data. The model will be of such a form as to facilitate an analytic proof of the system's security, and to provide an initial basis for security certification. 38

This abstract model will serve to define an isolated security-oriented "kernel" of an operating system. The kernel must be capable of protecting itself and key data bases from unauthorized access. It must be invoked (through the descriptors it controls) to check every access to information made within the system, and must be small enough so that its operation can be understood, tested, and certified. The remaining bulk of the system can be implemented without concern for security. Certain modules outside the kernel may fulfill security roles, but can operate under the protection of (and limited by) the security kernel. 39

As the security kernel is being defined, the design of a segmented virtual memory operating system will be restructured around the kernel. This modified design will accomodate to peculiar military requirements such as file classification/user clearance relationships, classified residue controls, audit trails, security officer interface, and subverter to verify security features. 40

b. In the second, or implementation phase, the certifiable kernel and the surrounding operating system will be implemented to demonstrate the validity of the model and techniques. This phase will involve computer program development by a combination of contractor and AFSC resources. 41

Beginning in the design phase, but more importantly in the implelentation phase, direct, hands-on access to appropiate computer system hardware is required for design restructuring and software development. This includes both remote terminal use and extensive access to the "bare" machine for operating system tests. 42

c. The third, or integration phase, involves several steps or levels of integration. The operating system software must be integrated with the security kernel. The kernel must be integrated with the front-end processor/crypto multiplexer. These integration efforts may, in some cases, overlap development of "peripheral" software subsystems. 43

d. The fourth, or test and evaluation phase will involve assessing the utility and security of the secure computer system. Paragraph 9.3.2 discusses test and evaluation. 44

9.3.1.2 Front-end Processor/Crypto Multiplexer 45

a. The first, or design phase, will involve identifying cryptographic and processor techniques appropriate to providing an integrated front-end processor/crypto multiplexer. NSA will participate in the cryptographic portions of the task, while the processor design will be based on a selective application of the virtual memory techniques and models developed by the first task to provide the necessary security within the front-end processor and at its interface to the central computer. 46

b. During the second phase, a front-end processor will be implemented, probably by programming an off-the-shelf small virtual memory computer. This computer will be tested in a stand-a-lone mode during the implementation phase. 47

c. During the integration phase, the front-end processor will be merged with the cryptographic devices and with the central computer. 48

d. Testing of the front-end processor/crypto multiplexer will require evaluation of communications security, radiation, and computer security features. Paragraph 9.3.2 dicusses test and evaluation. 49

9.3.1.3 Secure Terminals 50

a. During the design phase this task will empnasize the unit cost reductions possible by an integrated design for input/output, communications, and encryption functions, using medium scale integration technology. This design will carefully consider the functions (such as user identification, central key insertion, authentication) necesary to support overall computer system security. NSA will provide necessary support for the design and development of communications security equipment. 51

b. In the implementatio phase, hardware will be constructed to demonstrate the security of the integrated design techniques and to verify the operational acceptability of the interactive terminal interface. 52

c. The integration phase will assure interoperation of the terminal and cryptographic elements of the secure terminal. The completed secure terminal and the front-end processor will also be integrated during this phase. 53

d. The testing phase will involve evaluating the radiation and communications security characteristics of the secure terminal. 54

9.3.1.4 Application Engineering 55

a. During the design phase, required characteristics for a data management system for use in a secure environment and for a security surveillance system will be identified. Appropriate design requirements for interfacing these application aids to the central computer operating system will be supplied to the central computer design task. The data management and surveillance tool designs will be documented. 56

b. During the implementation phase, the data management and surveillance tools will be developed in a form appropriate to the secure operating system. The developed tools will be tested initially in an environment that simulates the secure operating system. 57

c. During the integration phase, the data management and surveillance tools will be merged with the secure operating system and kernel. 58

d. During the test phase, the computer security and utility of the data management and surveillance tools will be assessed. 59

9.3.2 Evaluation Criteria and Functional Tests: The communications security and radiation security of the front-end processor/crypto multiplexer and of the secure terminals will be assessed during the integration and testing phase. NSA and Air Force Security Services standards apply to these tests, and the participation of these agencies will be requested. 60

Computer security aspects of the central computer, front-end processor, and application engineering tools will, for the most part, be assured during design and implementation phases of the appropriate tasks. Independent assessment of the computer security will be requested of the ARPA-sponsored penetration groups at Rand Corp. and Lawrence Livermore Laboratory. These assessments will be performed during the test phase. 61

System utility will be assured by providing Air Force computer users with access to the secure computer system throughout the test phase. System and user response will be assessed from measurements and user reactions. 62

9.4 ADP SYSTEMS SECURITY 63

9.4.1 This task consists of four sub-tasks: central computer, application engineering, secure terminal, and front-end processor/crypto multiplexer. Each sub-task includes four phases: design, implementation, integration, and evaluation. 64

9.4.2 Schedules within Master Schedule 65

9.4.2.1 Documentation Schedule 66

1. DMS Design Contract	Jan 74	66a
2. Front-end Processor Contract	Jul 74	66b
3. Secure Terminal Design Contract	Jul 74	66c
4. Kernel Implementation Contract	Jul 74	66d

5. Progress documentation will be provided at the end of each phase 66e

9.4.2.2 Key Decision Points 67

These will occur at the end of each phase of each sub-task, as security criteria are developed and the validity of the approach is confirmed. 68

9.5 FINANCIAL (FUNDS X$000)

TITLE	PRIOR	FY-74	FY-75	FY-76	FY-77	FY-78	FY-79
Central Computer							
Abstract Model & Certification	200	300	200	-			
Security Kernel Design/Devel	365	150	60	-			
ADP Support	85	-					
Front-end Processor	150	350	-				
Applications Engineering							
Secure DMS	-						
Security Surveillance	50	100	-				
Secure Office Terminal	50	-					
TOTAL	900	900	260				

NOTE: THE ABOVE FUNDS DO NOT REPRESENT THE FUNDS AS DETERMINED BY THE TASK ENGINEER ,MAJOR SCHELL/ESD, AS THOSE BEING REQUIRED. HIS ESTIMATE IS HIGHER. THE PROJECT 5550 STEERING GROUP HAS DETERMINED THAT MOST OF THE WORK BEING PROPOSED FALLS WITHIN THE 6.4 AREA OF WORK. THEREFORE, THE GROUP HAS RECOMMENDED THAT THE WORK BE FUNDED IN THE 6.4 AREA STARTING IN FY-76 AND THAT WORK WHICH FALLS WITHIN ADVANCED DEVELOPMENT WILL CONTINUE TO BE FUNDED FROM THIS PROJECT IN SUPPORT OF THE ENGINEERING DEVELOPMENT SCHEDULED TO START IN FY76.

9.6 MANPOWER

FUNCTIONAL TITLE	AFSC	FY74	FY75	FY76
Computer Systems Staff Officer	5116	2	2	2
Computer Systems Design Engineer	5125B	2	3	3
Development Staff Officer	2816	1	1	1
Electronic Engineer	C2825B	1	1	1
Facility Manager		1	1	1
Computer Operators		-	2	3
Manpower Required		6	10	11
Manpower Available		3	3	3
Additional Required		3	7	8

NOTE: MANPOWER LEVELS AFTER FY76 TO BE DETERMINED. SEE NOTE UNDER FUNDS.

FY74 PMP TASK 09 SECURITY

(J20631) 29-NOV-73 12:31; Title: Author(s): Roger B. Panara/RBP;
Sub-Collections: RADC; Clerk: RBP;
Origin: <PANARA>FY74PMPTASK09SECURITY.NLS;1, 29-NOV-73 08:53 RBP ;

NDM 29-NOV-73 13:01 20633

Your SYSGD reformatting program

Dave: I tried your program on half a dozen sample statements from SYSGD. It is an interesting program. I looses statements without comments, of course. I'm not sure what could be done about that. Also, it would require the convention that the first word of each comment be a keyword. As I told you early in the game, we are considering how to handle the problem of indexing SYSGD and facilitating user use of L10 procedures. I will certainly keep this program in mind. Thank you. By the way, your programming looks excellent. I'm not sure if I'm going to be much help to you from here on, since you may know as much as I. I will ask your advice (early 1974) on the problem of making L10 a more useable and simple user programming language. --Dean 1

20633 Distribution
David H. Crocker,

Your SYSGD reformatting program

(J20633) 29-NOV-73 13:01; Title: Author(s): N. Dean Meyer/NDM;
Distribution: /DHC; Sub-Collections: SRI-ARC; Clerk: NDM;

Dirk: Your DDSI announcement looks fine. I assume spelling will be corrected before it goes out. I don't know what my extension will be when I'm back there full time, but it certainly would not be wise to advertise 4908 unless I can have that transfer to an office there. You might talk to Norton about the problem. --Dean 1

20634 Distribution
Dirk H. Van Nouhuys,

(J20634) 29-NOV-73 13:06; Title: Author(s): N. Dean Meyer/NDM;
Distribution: /DVN; Sub-Collections: SRI-ARC; Clerk: NDM;

Test Message

This is a test for NEWNLS

20635 Distribution
New Nls,

SRL 29-NOV-73 12:48 20635

Test Message

(J20635) 29-NOV-73 12:48; Title: Author(s): Susan R. Lee/SRL;
Distribution: /NEWNLS; Sub-Collections: SRI-ARC NEWNLS; Clerk: SRL;

EJK 29-NOV-73 13:53 20636

Supply Summary for Maintenance Purposes

Bobbie how's about running this out on your old TYCOM. Ifyou feel lucky, do it on bond. Viewspecs nw.

Supply Summary for Maintenance Purposes

ISIM (E. J. Kennedy/3827) 29 November 1973 1

2

ARPA Net Maintenance Support 3

4

RADC/ISFE (L. Comito) 5

6

In accordance with earlier correspondence (LJOURNAL,19855,1:w), (IJOURNAL,20365,1:w) and in reply to your memo of the same subject, (ijournal,20605,1:w) dated 21 November, the folowing is provided to serve as a basis for your planning. 7

8

Following is a list of current terminals and I/O devices acquired (or in the process of being purchased) under the AKW project, with an indication of supplies needed or on hand: 9

Execuport: 12 units, models 310&311, thermal print head, 10, 15 and 30 characters/second 9a

Supplies 9a1

Special heat sensitive paper available only from Computer Transceivers. It could also possibly be available from NCR (who makes the print head for CTI), but we have not investigated this. We have gone through the paper procurement route enough times so that standard paperwork is available. There are 319 rolls of this paper on hand and none is on order. 9a1a

Texas Instrument "Silent 700": 9 units, model 725, thermal print head, 10, 15 and 30 characters/second 9b

Supplies 9b1

Special thermal printing paper, available only from TI. There is none of this paper now available except partial rolls already in the machines, but we have ordered a pallet (528 rools) from TI. $4.25/roll FOB Stanford Texas....6-8 week delivery. 9b1a

IMLAC: 3 units, model PDS-1D, mouse, keyset, cassette recorder,

and long vector hardware options....also have one programmers console for debugging, programming purposes etc. 9c

Supplies 9c1

We could use another mouse or two as backup. We need a ready supply of cassette tapes. We currently have 30 of these on order, which should do us for the rest of this Fiscal Year. 9c1a

TYCOM: 5 units (2 here, 3 on order..arive by Dec), model 38KSR, IMB Selectric II typewriter + base plate + electronic box and acoustic coupler, 10 characters/sec, ASCII code. 9d

Supplies 9d1

The TYCOM does not require any special paper. Any roll paper is ok...sometimes we use bond for printout of final version of a document. It takes a cartridge type ribbon, which should be stocked if it already isn't being done. We would like to get a pin feed platen from IBM for some applications..about $125. We also need some additional type balls from IBM (ASCII). 9d1a

Termicette: 4 units, model 3000-3, digital cassette tape recorders, 10, 15 and 30 characters/sec..used to prpare off-line text tapes for input to SRI NLS. 9e

Supplies 9e1

A supply of tape cassettes will be needed once we get into full use of the units. The quantity should not be too great, since they are reuseable, but we don't know how many times. As previously stated there are about 30 cassettes on order. We have about 20 on hand. 9e1a

Line printers: two units (one-Data Products here, the other-Pertec on order) 9f

Supplies 9f1

There is still a need for a special kind of paper for one of the printers. It should be 132 columns wide, prepunched holes for a three ring notebook, perforated on the left side to allow removal of feed chain holes and perforated between the 80th and 81st column. 9f1a

10

Supply Summary for Maintenance Purposes

11

12

FRANK J. TOMAINI

Chief, Information Processing Branch

Info Sciences Division

13

14

15

20636 Distribution
Roberta J. Carrier, Duane L. Stone,

EJK 29-NOV-73 13:53 20636

Supply Summary for Maintenance Purposes

(J20636) 29-NOV-73 13:53; Title: Author(s): Edmund J. Kennedy/EJK;
Distribution: /RJC DLS(info); Sub-Collections: RADC; Clerk: EJK;